REMARKS

Applicants request favorable reconsideration and allowance of the present application in view of the foregoing amendments and the following remarks.

Claims 38-42, 45-50, 53-58, 61-66, and 69-77 are pending in the present application. Claims 38-41 are the independent claims.

Claims 38-41, 50, 58, 64, and 65 have been amended, and new Claims 74-77 have been presented. Applicants submit that support for these amendments can be found in the original disclosure and that no new matter has been added.

Claims 38, 39, 40, 41, 42, 45-47, 50, 53-55, 58, 61-63, 66, 69-70, and 73 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,611,599 (Natarajan). Claims 48, 49, 56, 57, 64, 65, 71, and 72 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Natarajan. Applicants respectfully traverse these rejections for the reasons discussed below.

As discussed in the background section of the specification (e.g., page 2, line 2 through page 3, line 7), one conventional system for checking whether digital data has been altered involves applying a hash function to digital data and then using a private key to encrypt the result of the hash function to obtain a digital signature. The digital signature is transmitted together with the digital data to a receiving device and can be used to verify the integrity of the received digital data. However, private key encryption requires complex mathematical operations and therefore requires significant process power to perform.

In contrast, the present invention as recited in independent Claim 38, includes the feature, *inter alia,* of a calculation unit to (a) perform a predetermined calculation using an encoded digital image and confidential information, wherein the predetermine

calculation does not include encryption using the confidential information, and (b) generate the additional data by applying a one-way function to a result of the predetermined calculation. In other words, the invention of Claim 38 first performs a predetermined calculation using confidential information, which does not include encryption using the confidential information, and then performs a one-way function. As a result, the integrity of data can be verified without the need for encryption that requires significant processing power.

Applicants submit that the cited art fails to disclose or suggest at least the above-mentioned feature. The Office Action asserts that the combination of the one-way hash function unit and the encryption key signature unit in Natarajan correspond to the claimed predetermined calculation using confidential information, and the watermark generating unit 106 in Natarajan corresponds to the claimed generation of additional data using a one way function. In support of this position, the Office Action cites the Abstract of U.S. Patent No. 6,209,092 as allegedly teaching that the function of deriving a watermark is a one-way function. Applicants respectfully submit that the cited portion merely indicates that the method of deriving a watermark in that patent uses a one-way function, and it does not teach that every watermark is generated using a one-way function. In particular, it does not teach that the method of generating a watermark used by unit 106 in Natarajan uses a one-way function. Moreover, the combination of the ne-way hash function unit and the encryption key signature unit in Natarajan cannot correspond to the claimed predetermined calculation using confidential information in Claim 38, as now presented, because the claimed predetermined calculation does not include encryption using the confidential information.

-11-

Accordingly, Applicants submit that the cited art fails to disclose or suggest at least the features of performing a predetermined calculation using a digital image and confidential information, wherein the predetermined calculation does not include encryption using the confidential information, and generating additional data by performing a one-way function on the result of the predetermined calculation, as recited in Claim 38. Therefore, that claim is believed patentable over the art of record.
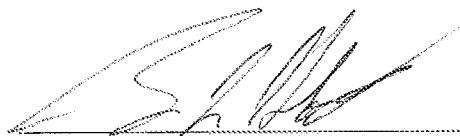
Independent Claims 39-41 are believed for reasons similar to Claim38. The dependent claims are believed patentable for at least the same reasons as the independent claims, as well as for the additional features they recite. In particular, Claims 74-77 recite that the predetermined calculation involves an exclusive-OR operation.

In view of the foregoing, this application is believed to be in condition for allowance. Favorable reconsideration, withdrawal of the outstanding rejections, and an early Notice of Allowance are requested.

If the Examiner believes there are any unresolved issues, he is invited to telephone Applicants' undersigned representative to discuss them in a telephone interview, in order to expedite prosecution.

Applicants' undersigned attorney may be reached in our Washington, DC

office by telephone at (202) 530-1010. All correspondence should continue to be directed

to our below-listed address.

Respectfully submitted,

Attorney for Applicants
Brian L. Klock
Registration No.36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/lmj
DC 171859v1

DC_MAIN 263382v1